

FAQ version 3.0



Contents

AVG CloudCare Installation 6

How do I deploy AVG CloudCare to devices?

AVG Antivirus 8

What firewall settings are available within the AntiVirus service?

How do I add specific files/folders/directories as exceptions?

How do I schedule an AntiVirus scan?

Will AVG remove competitive antivirus products before installing the AVG AntiVirus Service?

Will AVG CloudCare remove my existing AVG products before installing the AntiVirus service?

AVG Content Filtering 10

How to add sites to the Exception List?

What web browsers will AVG CloudCare support for the Content Filtering service?

What does the Content Filtering password allow you to do?

How long until an overridden site is blocked again?

AVG Email Security Services 12

How do I migrate my customer over to using the Email Security Services?

Is the AVG AntiSpam part of the AVG CloudCare platform?

Will I need to provide my payment details in the ESS portal?

Are there any Hardware or Software requirements needed to use AVG AntiSpam?

How do I get started with the AVG Email Security Services?

AVG Remote IT 13

Receiving connection issues when trying to remotely connect to a device?

What software is required in order to use Remote IT?

Troubleshooting issues with remote deployment

AVG Online Backup 16

What kind of encryption is used to protect the stored data?

What Operating Systems does the Online Backup Service support?

What are the minimum system requirements for the Online Backup Service?

What certifications are we covered by?

What government regulations are we covered by?

Where are the data centers located?

Will an NFR be available for the Online Backup Service?

Is there an option for continuous data backup?

How do you delete a backed up file?

With the all files and folders option, can you exclude or add file paths manually, such as ones that are hidden?

Will there be some type of user sensitive feature that will throttle the backup if the user is active at the time of a backup?

Is the backup plan per device or account?

ShadowProtect 18

What is ShadowProtect?

What operating systems does ShadowProtect support?

Will ShadowProtect image backups work when windows user is not logged in?



Can ShadowProtect run on a machine that has other softwares that use VSS?

How many versions of a file are kept, and how does that count towards the data limits?

How is the encryption key stored, is it stored in the cloud or local machine or both?

Policies and Devices 20

How do you move a device from one policy group to another?

How do you remove/delete a policy group or device group?

Alerts and Reporting 20

How do I deactivate an alert?

Can customer reports be automatically generated and scheduled to be sent via email?

Billing and Invoicing 21

Where can I find billing and invoicing information?

Help Files 21

User Manuals and Quick Start Guide

Release Notes

AVG Community Forum 21

I have an AVG CloudCare account, will I have access to the AVG Community Forum?





AVG CloudCare Installation

How do I deploy AVG CloudCare to devices?

Click the pull-down menu on the left side of the "Devices" interface and select "Add Device". Choose which option you would like to use to install the AVG CloudCare™ agent:

- Email Invitation for Download and install - with this option, you can send users an email with a link and instructions to download the AVG CloudCare™ agent installer.
- Create Redistributable Install Package - this option allows you to save the AVG CloudCare™ agent installer onto removable media for redistribution.
- Remote Deployment - this option allows you to remotely deploy the installer package to devices within your network.

 You must have already used another method for adding a device to your network before you can use the remote deployment option.

Option 1: Email Invitation for Download and Install

Click "Email Invitation". A separate dialog box will open allowing you to select which services you wish to install along with component selections. You also have the option to add a trial to selected services.

The second tab, "Send Email Invitation" or "Generate Download" Link will provide you with the following options:

- Send Email Invitation
- Generate Download Link

Send Email Invitation

Enter an email address of each user that should receive the install package. You will also have the option to Edit Email Content which will allow you to edit the body of the email and subject heading.

The body of the email will have a generic message instructing recipients to download and install the AVG CloudCare™ agent onto their machine.

To view the status and history of all emailed invitations sent, go to the "Email Device Deployment Report".

Generate Download Link

This option will allow you to generate a download link for selected services which you can then copy and paste into your own e-mail application to send to a users email address.



Option 2: Create a Redistributable Install Package

Click the Download button and save the installer package onto a CD or flash drive. Install onto each device directly or push to machines within your domain through Active Directory (if available).

Option 3: Remote Deployment

Click 'Start' to launch the Remote Deployment wizard, which will guide you through the following steps:

Select Services to install

1. Tick the services that you wish to deploy to the devices in the "Select Devices" tab.
2. Click 'Next' to proceed to the next step. Click 'Cancel' to exit the wizard and return to the portal.

Select Devices

1. Click on a WAN IP address to expand and view the name, IP address, and installation state of each discovered device. Devices already in the AVG CloudCare™ network will show the version of AVG CloudCare™ installed and the device group to which they belong.
2. Click 'Next' to proceed to the next step. Click 'Cancel' to exit the wizard and return to the portal.

Scan Network

1. Add the names and passwords of all possible network administrators to the list of accounts. This list is saved by default and will reappear each time you initiate the remote deployment option. If you do not want to save the current list, uncheck the box next to Save list of accounts before proceeding. If adding a domain administrator you must use the syntax of (yourdomain\domainadmin) otherwise remote deployment will fail.
2. Click 'Next' to proceed to the next step. Click 'Cancel' to exit the wizard and return to the portal.

Confirm

1. Check the device(s) that you are deploying the AVG CloudCare™ agent to.
2. Click 'Deploy' to complete the deployment of the agent to each of the selected devices.
3. Click 'Back' to go to the previous step.
4. Click 'Cancel' to exit the wizard and return to the portal.

To view the installation progress, visit the "Remote Device Deployment Report"



AVG Antivirus

What firewall settings are available within the AntiVirus service?

In the "Firewall Settings" section you can change the firewall status as needed:

- Firewall Enabled - select this option to allow communication to those applications that are assigned as 'allowed' in the set of rules defined within selected Firewall profile.
- Firewall Disabled (default) - this option switches Firewall off completely, all network traffic is allowed but not checked.
- Emergency Mode (block all Internet traffic) - select this option to block all traffic on every single network port; Firewall is still running but all network traffic is stopped.

If Firewall 'Disabled' option is used for a policy, the end user will not receive any firewall prompts.

 If you do not wish to use the AVG Firewall during deployment options 1, 2 and 3, you will have the option not to install the AVG Firewall. By default the AVG Firewall is not installed.

How do I add specific files/folders/directories as exceptions?

 Please always make sure that the file or program in question is absolutely safe!

To exclude a file or folder from the Resident Shield detection:

1. Go to the Policies tab
2. From the Policies tab, click on the 'AntiVirus' heading.
3. In the sub tab pane, select 'Exceptions'.
4. Click 'Add exception'.
5. In the drop-down menu, select exception type – File, Folder or URL.
6. Browse to the file or folder that you want to exclude.
7. Select whether you want to apply the exception also for other AVG components.
8. Click 'Save' to save details of the exception.

How do I schedule an AntiVirus scan?

To set an automatic scan of your computer:

1. Go to the 'Policies' tab.
2. Click on the 'AntiVirus' tab.
3. Click the 'Scan Settings' button.
4. Click 'Scheduled Settings'.
5. Click on 'Enable Scheduled Scan' to activate the scan, there should be a check mark in the check box.
6. Fill in the scan details.
7. You can also access additional settings by clicking 'Advanced Settings' at the bottom.
8. Click 'Save' to apply the settings.

Will AVG remove competitive antivirus products before installing the AVG AntiVirus Service?

Yes, AVG Cloudcare does remove competitor products. The following AntiVirus products are not supported for removal by AVG CloudCare:

- Avast! 7.0.1455+
- Vipre 5.0.4959+
- GFI Vipre Business 5.0.4959+
- FSecure 2013
- BitDefender 16.16.0.1348
- Symantec Endpoint Protection Manager 12.1.1101.401

 The following AntiVirus products produce an error upon removal by AVG CloudCare:

- McAfee 11.6+ - Uninstalls McAfee but leaves NIC drivers
- Avira 12.0.0.1504+ - Can show unspecified error
- Norton Internet Security 20.1.0.24+ - Can cause the Norton feedback page to appear and then freeze

Will AVG CloudCare remove my existing AVG products before installing the AntiVirus service?

AVG CloudCare™ has the ability to remotely uninstall AVG versions 9.0, 2011, AVG 2012 and AVG 2013 Business Editions and, Home products silently before installing AVG CloudCare™ services.

AVG Content Filtering

How to add sites to the Exception List?

On the Policies tab, select the policy you would like to manage.

- Click on 'Content Filtering Settings' to expand the menu.
- Select the 'Exceptions' tab.
- Type the URL of the site into the "Blocked" or "Allowed" websites list and click Block or Allow to add to the list.
- Click 'Save' to save your settings or 'Reset' to cancel any changes.

 Checking the "Only allow sites listed in the Allowed list" will ONLY allow access to the sites listed on the Allowed websites list.

What web browsers will AVG CloudCare support for the Content Filtering service?

The AVG CloudCare™ Web interface supports the following browsers with the Adobe® Flash® Player 10.x plug-in installed:

- Internet Explorer 7.0 or later
- Firefox 2.0 or later
- Google Chrome - any version
- Safari 4.0 or later
- Opera 9.5 or later

Content Filtering options

The "Options" section in the Policies area allows you to manage the following Content Filtering settings:

- Clean Search - allows you to manage the built-in safe search feature of the Google, Yahoo and Bing search engines. Administrator Password - once enabled this allows you to create a local password to override blocked pages. Only the override password can be used to unblock sites.
- Safety Lock Option - This option is used to protect against users accessing multiple blocked sites. It prevents attempts to bypass filtering by forcing the user to restart their machine after a specified number of attempts have been blocked. The threshold is set on a scale from 1 to 10, where 1 means the user can be blocked in 16 out of the last 16 URLs before having to reboot the machine and 10 means that the user can be blocked in 3 out of the last 16 URLs before having to reboot the machine to access the Internet again.
- iCat Dynamic Filtering - provides a second line of defense against uncategorized sites. If a site contains adult or mature content, it will be blocked.



What does the Content Filtering password allow you to do?

This option allows you to create a secondary, local password to override blocked pages without compromising the administrative password. Both the AVG CloudCare™ administrator password and this local policy password will work to override blocked websites.

How long until an overridden site is blocked again?

If you temporarily override a site it will be allowed for up to 24 hours. This cache is cleared once a day when the device checks in. You can clear the cache manually by holding CTRL and right clicking on the tray icon, click clear cache.

Go to Webinar/Meeting/Assist when the Content Filtering service is activated

This does not always need to be done. In a number of cases GoToAssist will pick another port if it cannot connect and resolve this on it's own. However, we have observed situations similar to this in the past and used the following to resolve it.

We are happy to assist you with configuring GoToAssist to work properly with CloudCare.

1. Visit <http://www.gotoassist.com/wizard/>.
2. Click on "GoToAssist Connection Wizard".
3. Click "Run" (if using firefox, make sure to double click g2wizard.exe).
4. Click "Yes" on the box that asks to allow gotomypc to make changes.
5. When the wizard opens do not click the button that says "Run Wizard" You will know when you see this window as it will have a green bar across the top of it. When you see this Right click in the right side of the green bar.
6. Click "Manual Tools" at the bottom.
7. Click "Reset", then click "Reset" again on the popup to confirm.
8. Click "Ok".
9. Now click "Custom wizard".
10. Uncheck "Enable Dynamic Proxy Detection".
11. Click "Next".
12. It will now run a connection wizard, this takes a few minutes and will run a series of tests. When this is complete click next.
13. Now make sure that you select Direct, HostPort: 8200 (When configuring GoTo please see workaround below).
14. Click the drop down menu in the bottom right and set it to 'force'.
15. Make sure that the other 2 options say 'None' under usage.
16. Now click "store new settings" twice.
17. Click "exit wizard", then reboot your computer & try GoToAssist.

Workaround for step 13 / GoTo Meeting

1. Click "add" at the bottom.
2. In target Host/Server port enter 8200.
3. Click "verify".
4. Now continue to step 14-> to finish. If you receive an error disregard it.

AVG Email Security Services

How do I migrate my customer over to using the Email Security Services?

Migration is very simple, it just requires you to change over your customers MX records to point to the AVG Email Security service. Full instructions on how to do this are located at AVG Email Security Service documentation.

Is the AVG AntiSpam part of the AVG CloudCare platform?

AVG AntiSpam service currently has a separate login portal to AVG CloudCare. You will have your login details for AVG CloudCare and separate login details for AVG AntiSpam service.

Will I need to provide my payment details in the ESS portal?

No, the invoicing and billing is carried out via AVG CloudCare as for the other cloud services.

Are there any Hardware or Software requirements needed to use AVG AntiSpam?

No hardware or software changes or requirements are needed. It requires the customers MX records to be changed. More information on this can be found in the AVG AntiSpam support documents, located on the AVG CloudCare forums.

How do I get started with the AVG Email Security Services?

Log in to your AVG CloudCare partner portal and there will be a new link: "Manage Email Security Services" in the customer summary area. Complete the registration page to sign up.



AVG Remote IT

Receiving connection issues when trying to remotely connect to a device?

We suggest allowing the following ports with both UDP and TCP. Also, allow traffic from the following IP Addresses.

Ports - both UDP and TCP 80, 443, 5222, 5911, 5910, 4931, 4930, 4932

IP Addresses:

- 204.193.144.88 204.193.144.90
- 204.193.144.91 204.193.144.92
- 204.193.144.93 204.193.144.94
- 204.193.144.95 78.47.220.186

The ports and IP addresses above should facilitate unrestricted access for authentication and Remote IT

I am receiving a constant "The AVG Remote IT service was not detected or needs to be updated. Install latest version now?" message when attempting to connect to a device.

After you install or update the Remote IT for the first time, please click on the "Refresh" button within CloudCare (not the browser) and then click on the "Connect" button, it should connect without the prompt.

What software is required in order to use Remote IT?

Java is needed in order for the Remote IT service to function correctly, please make sure that Java is installed on the host machine before attempting to connect to the device.

Troubleshooting issues with remote deployment

If the operating system of target PC is Windows XP, check following (and modify if it does not correspond):

Start -> Settings -> Control Panel -> Administrative tools -> Local Security Policy -> Security settings -> Local Policies -> Security Options -> Network Access: Sharing and security model for local accounts:

- default value: local users authenticate as guests
- new value: local users authenticate as themselves

To prove this:

- Open Start -> Run item on source computer
- Enter path \\<target_machine_name>\C\$. (Example: \\tester\c\$)
- Press enter. Open Winnt folder and try to save any file in there. If this is not possible, you do not have access to the C drive on target machine.

If you are unable connect to the remote computer, check the following settings:

1. Check your firewall settings

Windows Firewall (XP):

- Allow Remote Administration on remote computer

Execute NETSH command:

- netsh firewall set service RemoteAdmin enable

Or use Group Policies:

1. Run gpedit.msc
2. Navigate to Local Computer Policy >> Computer Configuration >> Administrative Templates >> Network >> Network Connections >> Windows Firewall
3. If the computer is in the domain, then choose Domain Profile; otherwise choose Standard Profile
4. Right click on Windows Firewall: Allow remote administration exception >> Properties
5. Click Enable, and then click OK

Open the DCOM and RPC ports

Execute NETSH commands:

```
netsh firewall add portopening protocol=tcp port=135 name= TCP135
```

```
netsh firewall add portopening protocol=udp port=135 name= UDP135
```

Windows Firewall (Vista/7)

Enable WMI traffic:

Execute NETSH command:

```
netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes
```

Enable DCOM

1. Run dcomcnfg
2. Navigate to Component Services >> Computers
3. Right click on My Computer >> Properties
4. Click the Default Properties tab
5. Tick "Enable Distributed COM on this Computer" check box

Enable RPC

1. Run services.msc
2. Navigate to "Remote Procedure Call (RPC)" and enable it

Disable Simple File Sharing (Windows XP)

1. Go to My Computer >> Tools >> Folder options
2. Open tab View
3. Uncheck "Use Simple File Sharing (Recommended)" check box

Enable ADMIN Share (Windows 7)

1. Open Regedit
2. Navigate to HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
3. Create a new DWORD "LocalAccountTokenFilterPolicy" with Value of 1 and enable Printer and file Sharing in Control Panel >> Network and Internet >> Network and Sharing Center >> Change advanced sharing settings >>> File Printer Sharing.



AVG Online Backup

What kind of encryption is used to protect the stored data?

Online Backup protects your data locally with 256-bit AES encryption, transfers over to the data center servers over a 128-bit SSL connection. Data is then secured at the data center with 1,024-bit AES encryption.

What Operating Systems does the Online Backup Service support?

- Windows XP® (32/64 bit versions of Professional, Home, Media Center SP2 or higher)
- Windows Vista® (32/64 bit version)
- Windows 7 (32/64 bit version)
- Microsoft Windows 8® (32/64 bit version)
- Windows Server 2003
- Windows Server 2008
- Windows Server 2011

What are the minimum system requirements for the Online Backup Service?

500MHz processor, 30MB free hard drive space and Microsoft .NET Framework 3.5 or higher is required for installation.

What certifications are we covered by?

ISO9001 Certified and ISO27001 Certified

What government regulations are we covered by?

- PCI
- HIPAA
- SAS 70 Type II (Sarbanes-Oxley)
- SSAE 16
- US EU SafeHarbor

Where are the data centers located?

We have data centers in the US and UK.

Will an NFR be available for the Online Backup Service?

Unfortunately, there will be no NFR available for the Online Backup Service at this moment in time.

Upon the next backup, will it drop the previous backed up file and replace it or only record the changes in order to reduce storage and bandwidth? How does that count towards the set limit of backup?

AVG Online Backup always uses differential backup. Files that have not changed are not backed up. If there is a change, the new version is uploaded. Usage is always calculated based on the largest single version of a file.

Is there an option for continuous data backup?

AVG Online Backup runs on a schedule or on demand.

How do you delete a backed up file?

Please follow the step by step instructions below to delete backed file(s) from AVG online backup.

1. Open the AVG Online Backup End-point Client by right clicking on the AVG CloudCare system tray icon. Select "Open AVG Online Backup Beta" from the popup menu. You will be prompted for the password you created during account creation.
2. Click on the 'Restore' tab. Press the 'Restore' button in the Restore My Files section, then click on the 'Online Restore' popup.
3. Select a date from the calendar, then press 'Next'.
4. Right click on the file or folder and select 'delete' from the popup menu.
5. To delete multiple files or folders at the same time tick the box next to each file, then right click on a file and select the 'delete' option.
6. Press 'Yes' on the confirmation window.

With the all files and folders option, can you exclude or add file paths manually, such as ones that are hidden?

Yes, you can manually add or exclude any files from being backed up.

Will there be some type of user sensitive feature that will throttle the backup if the user is active at the time of a backup?

Not at this time.

Is the backup plan per device or account?

Allocation is per customer account.



ShadowProtect

What is ShadowProtect?

ShadowProtect™ is StorageCraft's backup and disaster recovery solution for Windows. It allows the users to schedule (or manually create) frequent, image-based backups of their local disks and store them on disk-based or network destinations. The backup images include all files, settings, programs and operating system files on the volume, and are an exact representation of the entire volume at the time the backup was created.

What operating systems does ShadowProtect support?

ShadowProtect Server supports the following operating systems:

- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003 R2
- Windows Server 2003
- Windows Server 2000 (support is limited: ImageReady and VirtualBoot do not support 2000)

Note: All 32 and 64 bit operating platforms are supported.

Will ShadowProtect image backups work when windows user is not logged in?

Yes, the ShadowProtect service runs as a Local System user, and does not require anyone logged into the machine.

Can ShadowProtect run on a machine that has other softwares that use VSS?

No other software using VSS should be running when using ShadowProtect on that machine. No built in Windows Server Backups should be scheduled to run either.

How many versions of a file are kept, and how does that count towards the data limits?

All versions are kept. The usage is calculated based on the largest size.

How is the encryption key stored, is it stored in the cloud or local machine or both?

Data encryption key is stored on one of our servers in AES-encrypted form.



ShadowProtect job fails within a few seconds of starting the first full image and never completes.

This can occur if bad registry keys are not being replaced/removed from a previous install. To resolve this issue complete the following steps:

1. Download the PsExec which is included in the PSTools Suite: <http://technet.microsoft.com/en-us/sysinternals/bb897553>.
2. Extract PsExec.exe from the zip file, PSTools.zip.
3. Hold the Windows logo key and the "R" key at the same time to launch the Run prompt.
4. Execute the following command in the Run prompt: PsExec.exe -i -s cmd.exe (Make sure to enter the full path to the PsExec.exe file that was extracted in Step 2. You should see the command prompt launch, which will be running as the SYSTEM account. You will also see another command prompt launch that will show the version number of PsExec, this command prompt will not be used and can be minimized). The following steps will all need to be executed using the command prompt that was started by PsExec.
5. Within the command prompt, browse to the ShadowProtect installation directory. If you installed ShadowProtect to the default location, you can enter: cd "C:\Program Files (x86)\StorageCraft\ShadowProtect".
6. Enter: Stcinst -w (This cleans out bad registry keys. It may return errors that is ok).
7. Reboot.
8. Follow Step 4 again, browse to the installer of ShadowProtect and execute it within the command prompt. Select the "Repair install" option.
9. Reboot. Follow Step 4 and Step 5. Then enter: Stcinst -u (Uninstalls the drivers associated with ShadowProtect).
10. Reboot.
11. Follow Step 4 again, browse to the installer of ShadowProtect and execute it with the command prompt. Select the "Repair install" option.
12. Reboot.

Policies and Devices

How do you move a device from one policy group to another?

To drag-and-drop, left click and hold on the device name while you move the mouse. When it is at its new location, let go of the mouse button.

How do you remove/delete a policy group or device group?

1. Select the group on the Devices interface that you would like to remove.
2. Click the "Delete Group" option located above the table of devices.
3. Click "Yes" on the confirmation dialog to delete the group. Click "No" to cancel. All devices in the removed group will automatically be moved to your Default device group.

Alerts and Reporting

How do I deactivate an alert?

To deactivate an alert you will need to log into your AVG CloudCare™ account and click on the customer you wish to manage.

1. Click on the 'Alerts' tab
2. Locate the alert that you are deactivating on the Alerts table.
3. Under the Actions column, click the "Deactivate" action to stop monitoring the alert.

Can customer reports be automatically generated and scheduled to be sent via email?

Yes, and this can be easily set up by following the steps below:

1. Under your Customer Dashboard, click on the 'Reports' tab.
2. Click on the 'Schedules' sub tab.
3. Click on 'New Schedule' button.
4. Define your report.
5. Define your schedule.
6. Enter your recipients email addresses.
7. Click on 'Save' to finalize the schedule.

Billing and Invoicing

Where can I find billing and invoicing information?

Detailed billing and invoicing information can be found on the AVG CloudCare forums.

<http://community.cloudcare.avg.com/topic/150-new-cloudcare-pricing-information/>

For additional assistance, please contact your AVG CloudCare Account Manager:

- UK/Ireland - +44 1636 658 016
- North America - 866-833-5727
- Australia - 1300 284 000
- New Zealand - 0800 284 000

Help Files

User Manuals and Quick Start Guide

The AVG CloudCare User Manual can be found here: https://cloudcare.avg.com/docs/Cloud-Care_User_Manual.pdf

The AVG CloudCare Quick Start Guide can be found here: https://cloudcare.avg.com/docs/Quick_Start_Guide.pdf

Release Notes

All AVG CloudCare build release notes are sent via email communication and are also posted on the AVG Community forum under the 'Release Notes' category.

AVG Community Forum

I have an AVG CloudCare account, will I have access to the AVG Community Forum?

Yes, if you have an AVG CloudCare account you may access the AVG Community Forum. To access, log into AVG CloudCare and in the top right hand corner you will see "AVG Community" link. Click on this link and you will be presented with some mandatory fields in which you will need to fill in. After you have entered this information, the forum will use single sign-on which will use your AVG CloudCare login details.